Robert Stewart

Digfor inc  123 fake Street

Digital Forensics CA4 LAptop INvestigation

# Letter of Engagement

Modial LTD,

Dublin Rd,

Dundalk

Co. Louth

Friday, November 1st , 2019

Dear Mondial LTD,

Thank you for contacting DigFor Inc on Tuesday, October, 29th 2019 regarding the alleged theft of copyrighted digital material by an employee. We are happy to carry out the following on your behalf:

Acquire a forensic bit-stream copy (image) of the USB device currently in your possession. You have advised us that the USB device is a 4GB Transcend device and that this unit is the property of Mondial LTD. You have further advised us that the USB device may have been overwritten and consequently some of the data thereon may have been overwritten.

To establish and maintain a chain of evidence for evidential USB images and any evidential data recovered.

To examine the file system and unallocated spaces of the USB device to determine if any data, specifically a database, has been recently stored or erased from the USB device.

To determine as far as practical which data, if any, has been stored on, or erased from the evidential USB key.

To carry out a detailed assessments whether or not the evidential USB device was used for purposes contrary to the Mondial business interests

Following up on this an investigation on a company laptop will take place, the USB that has been previously examined is believed to be strongly linked to the negative activity on this laptop.

To produce a report of our findings.

We will commence this engagement on Friday, November 1st, 2019.

We will endeavour to submit a report setting out our activities and findings no later than Friday, November 13th, 2019.

You will understand that any delay in providing us with access to relevant information systems, or to information relevant for our consideration may affect our ability to conduct our analysis or to deliver our report within the agreed timetable.

Mr Dig For will act as the expert in matters of IT forensic analysis should testimony in court be required. The expert shall base their opinion on information provided to them and, unless otherwise agreed, will not seek independent confirmation. If that information is accurate or incomplete, or if the Expert is provided with further information, the Expert may need to change their opinions.

We will provide the work set out in the scope of work above for a fee not to exceed €1500 (ex VAT). We will not exceed this figure without prior permission of Modial LTD

Every effort will be made to protect the property of Mondial LTD, you should be aware that on very rare occasions USB devices fail under copying.

We reserve the right to decide what is reasonable or practical, given the fee and timescale involved.

If evidence is found on the USB device, that is required by law, to be reported to the authorities then we will do so immediately.

By signing this letter of engagement you warrant that you are authorised to give us access to the data and that you agree to all the terms and conditions set out herein.

Signed by or on behalf of the client

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date \_\_\_/\_\_\_/\_\_\_\_\_\_

# Terms & Conditions

* Our fees and invoicing arrangements
* Our responsibilities to you
* Your responsibilities to us
* Information and confidentiality
* Electronic communication
* Limitation of our liability
* Data protection and privacy
* Intellectual property rights
* Force Majeure
* Severance of terms
* Governing law and jurisdiction
* Investment Business Regulation
* Statutory and regulatory obligations

# Table of Contents

[Letter of Engagement 1](#_Toc27168433)

[Terms & Conditions 2](#_Toc27168434)

[1. Table of Contents 3](#_Toc27168435)

[2. Introduction: 4](#_Toc27168436)

[3. Tools Used: 4](#_Toc27168437)

[4. Methodology 5](#_Toc27168438)

[5. Conclusion 13](#_Toc27168439)

# Introduction:

Following up the investigation that was launched in Mondial ltd regarding the potential theft or destruction of sensitive information through the user account of Frances Byrne, using the now well documented Transcend 4GB USB device, follow up suspect evidence has been handed over by Mondial ltd in the form of a laptop which has allegedly been used by the Frances Byrne employee account.

An image of the laptop will be taken and an investigation will be carried out an all evidence of foul play with the companies sensitive information will be documented.

# Tools Used:

* Razer, 8th Gen Intel Core i7-8750H processor, 6 cores/12 threads, 4.1Ghz, 16GB RAM, GTX 1060.
* Autopsy (Version 4.12.0)
* Access Registry Viewer (Demo Mode)
* Decode (Version 4.02a)
* USB View
* Win Prefetch View

# Methodology

The user Frances’WorkPC is confirmed to have been logged into this laptop at some point in time.

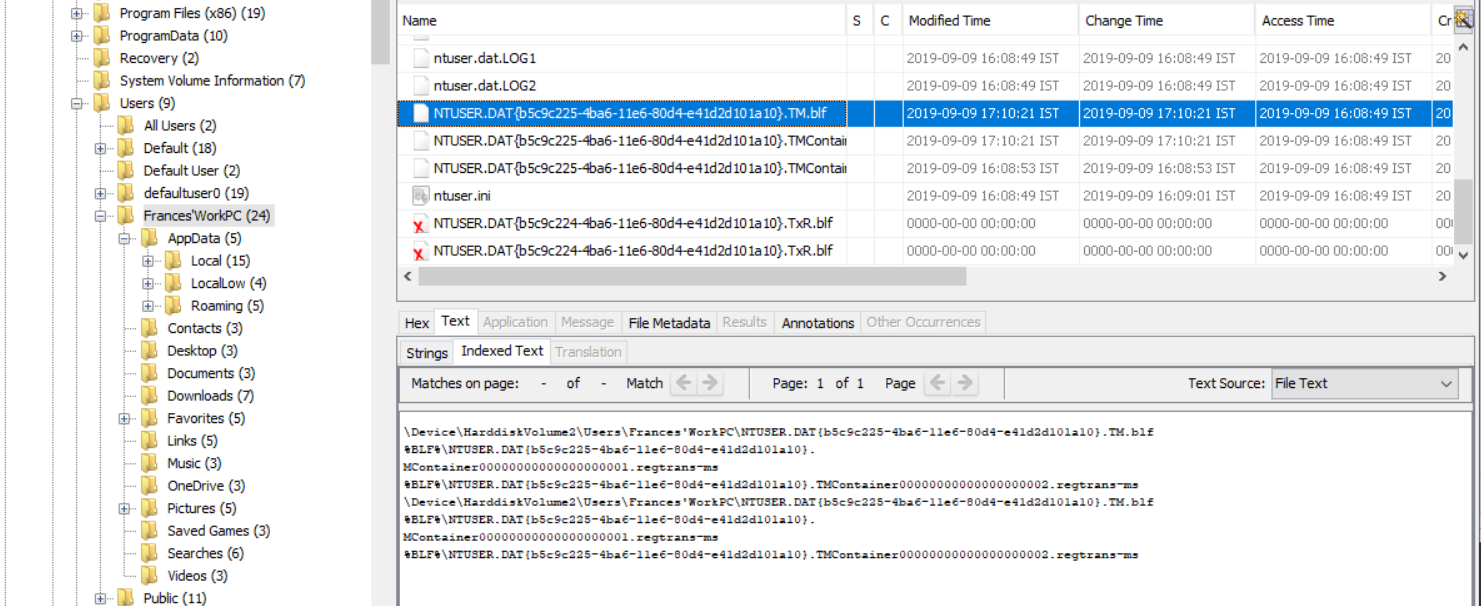
T

Figure . Evidence of the user Frances Byrne

Microsoft Access has been executed on the laptop with modifications being applied at approximately 17:28 UTC, on the 9th of September 2019.

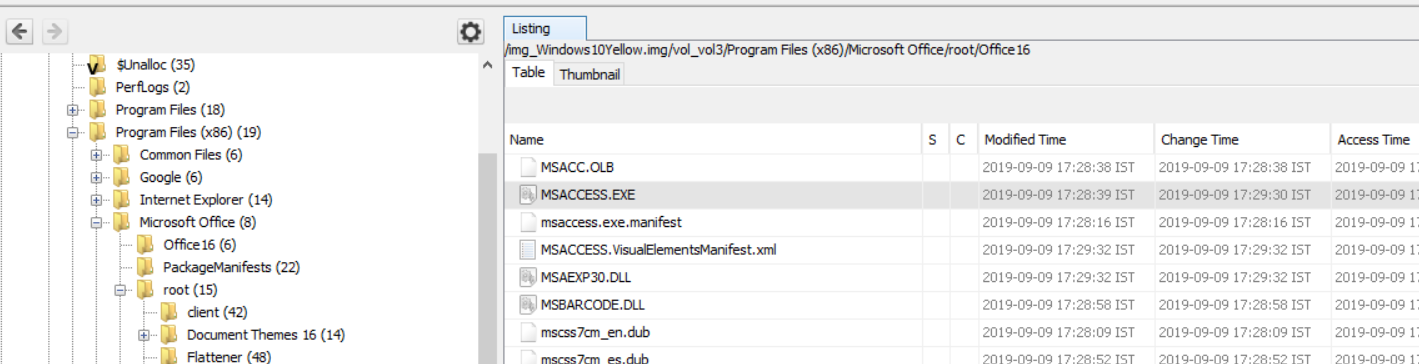


Figure . Access activity found.

Further investigation has uncovered the database which was moved to the Recycle Bin on the 6th of October at 21:09 UTC.

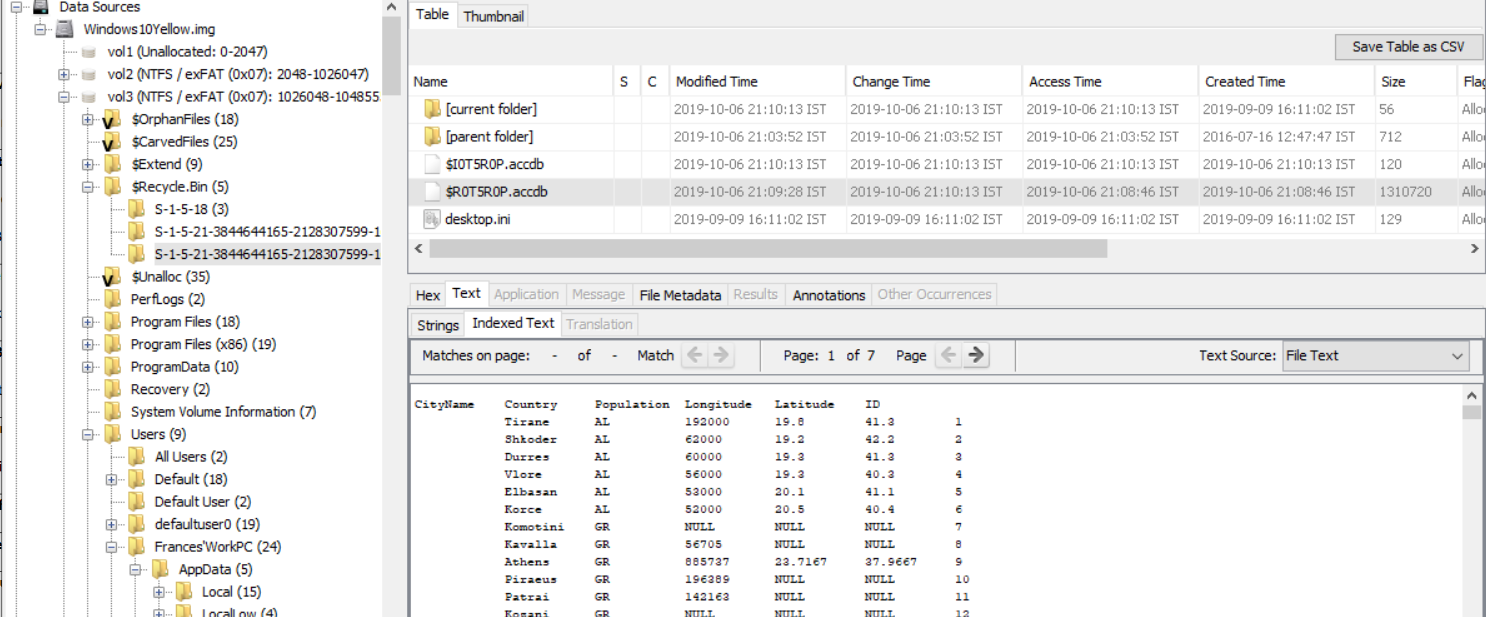


Figure . Database was deleted and found in recycle bin

After extracting the Storage Area Management (SAM) file, the user Frances Byrnes SID and last login time were discovered.

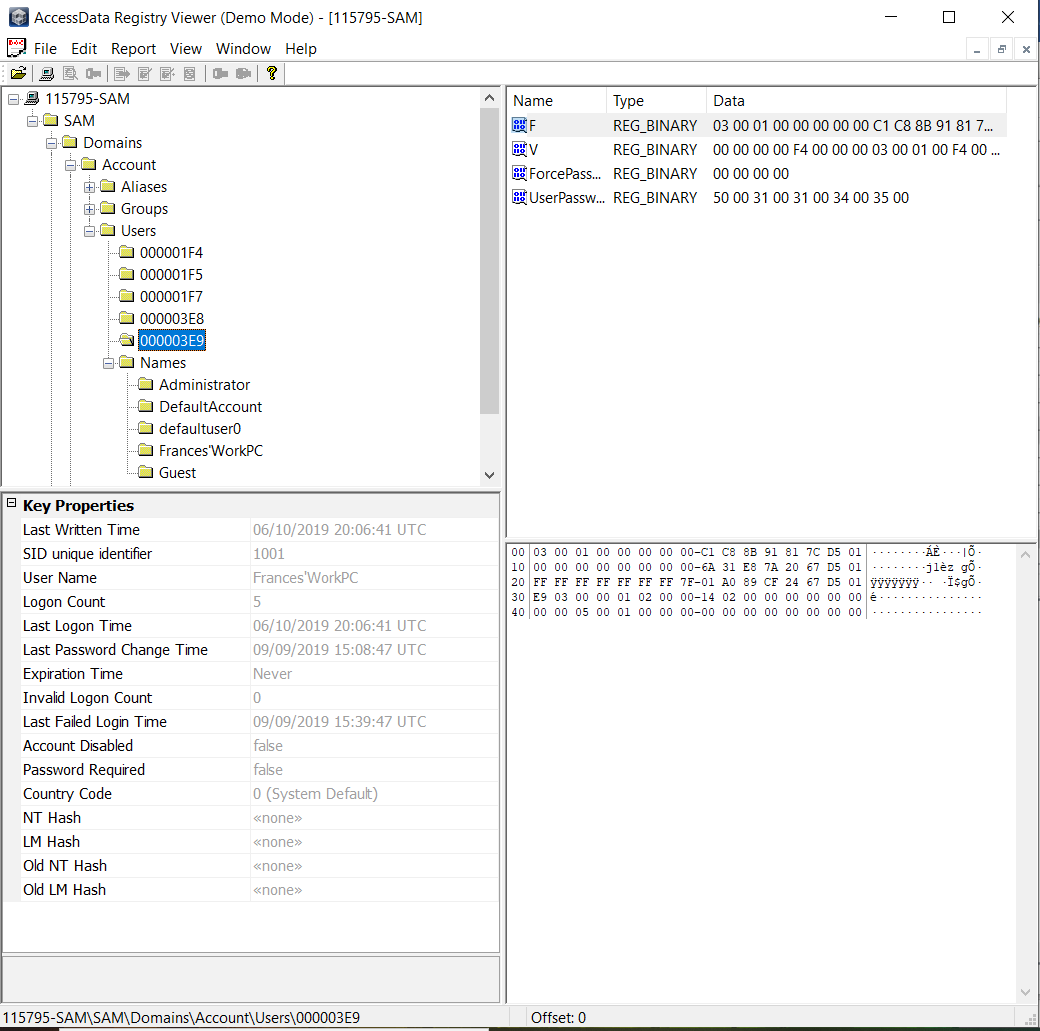


Figure . Overview of discovered data

In this zoom in on figure 4.3 the SID unique identifier and last login time are clearly visible.

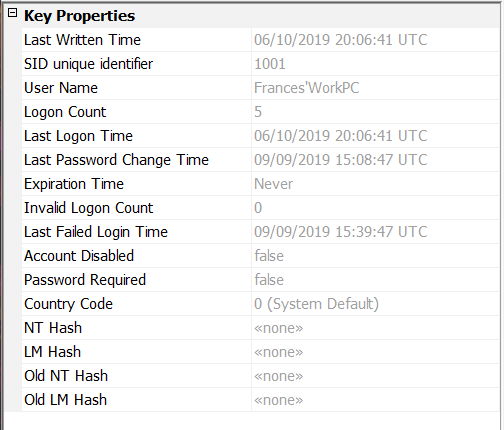


Figure . SID and last login time

The user FrancesWorkPC is clearly linked to the hexadecimal 000003E9 number folder, with in which all the details from figure 4.3 were discovered.

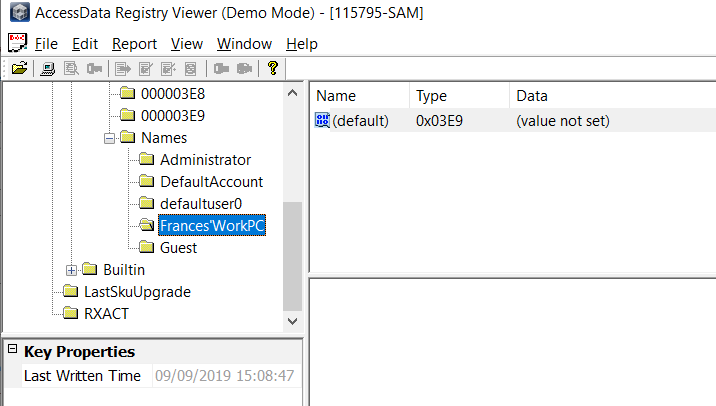


Figure . Matching hexadecimal values

The following shows timezone information, the Bias shows that daylight savings is active and the DaylightBias show a hexadecimal number FFFFFFC4, which is a negative number and when transformed into decimal is -60. This is very important to note considering the laptop is storing everything in UTC by default, any activity prior to the last weekend in October with UTC in the timestamp must have an hour added to it to reflect the current time of day when these actions were carried out.

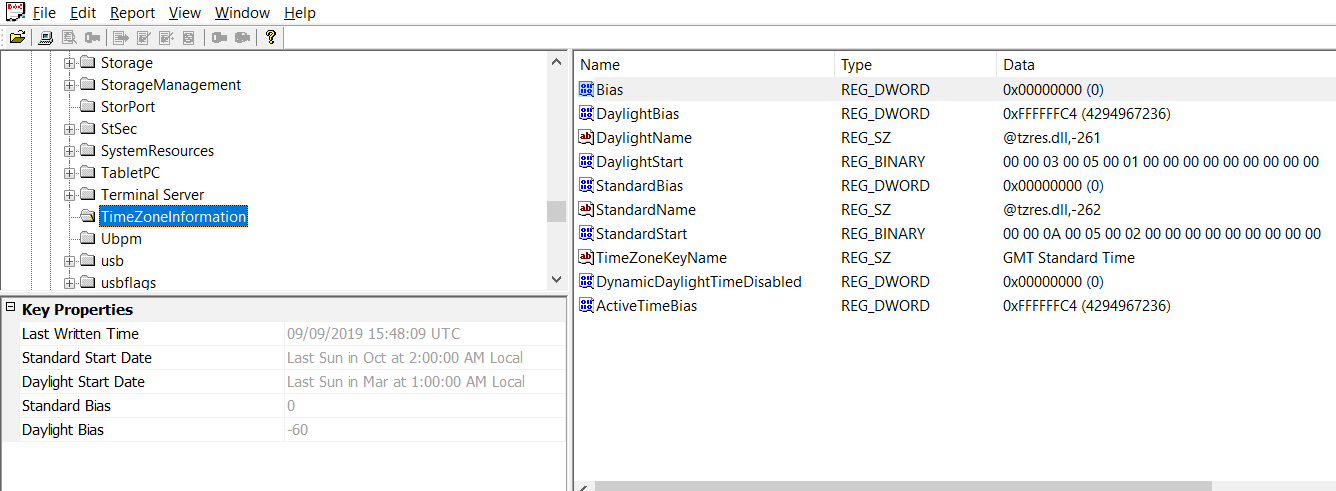


Figure . Shows TimeZoneInformation and Daylight savings

Within this parameters folder the Network Time Protocol (NTP) can be found, this laptop is using windows time.

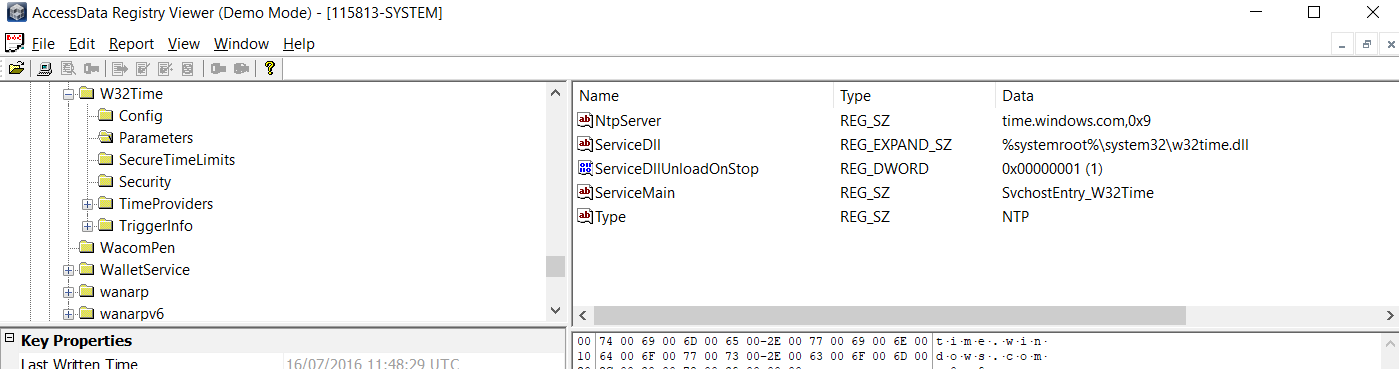


Figure . NTP Information

The systems shutdown time was found in the Windows directory under control and controlSet. The time is only stored in Hex through this view.

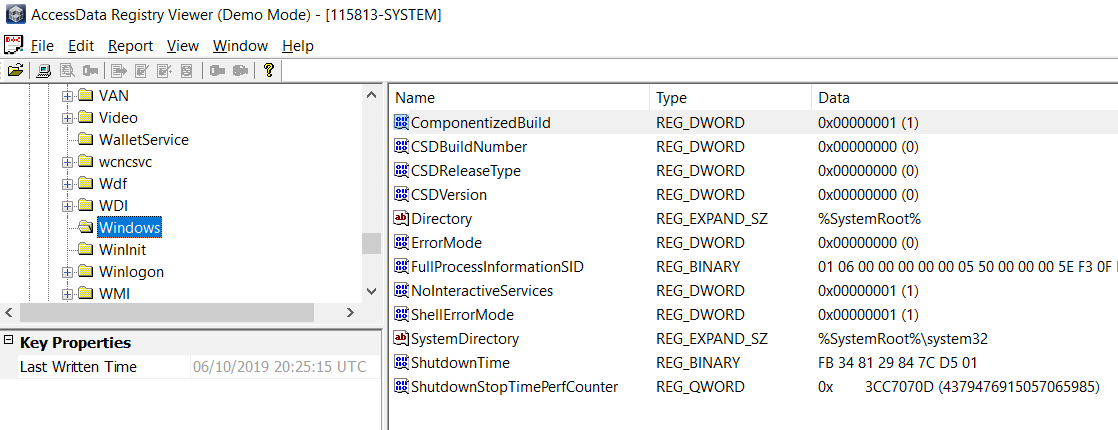


Figure . Laptop Shutdown time

Using the software Dcode, a human readable time format was obtained, note that it is in UTC.

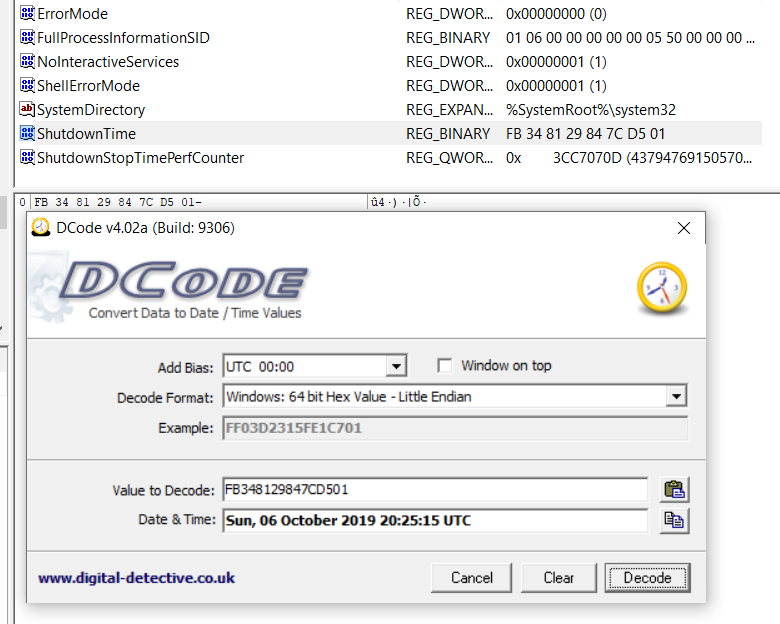


Figure . Shutdown time in human readable format

In the extracted SYSTEM file, evidence of the 4GB USB has been found. Its serial number is highlighted blue in figure 4.10 left side window. The last written time visible in the bottom left side window was 20:00:04 UTC

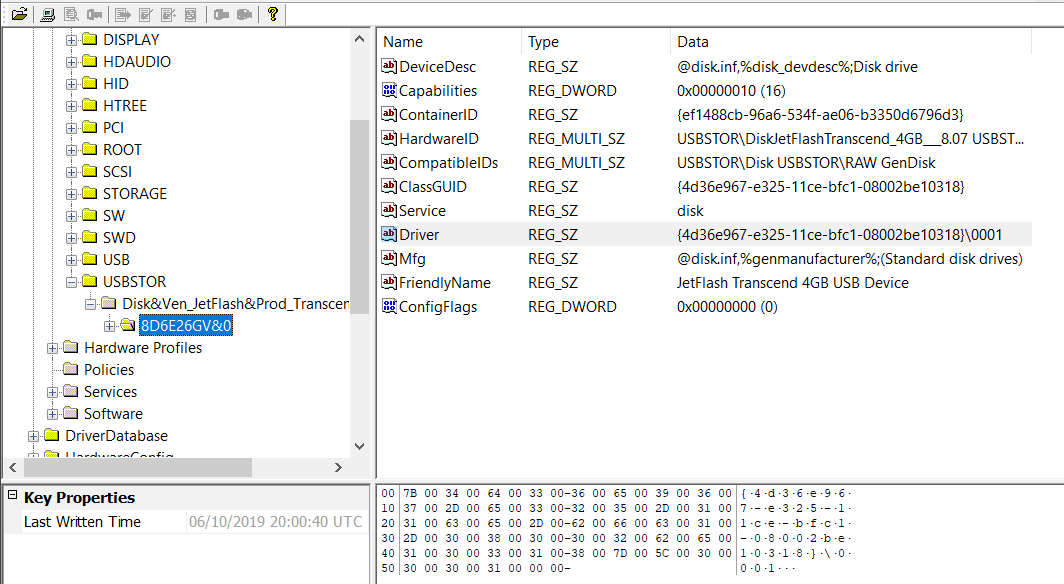


Figure . Evidence of USB

Through USBView it can be seen that the 4GB Transcend USB does match the USB that has been found on the laptop in figure 4.10.

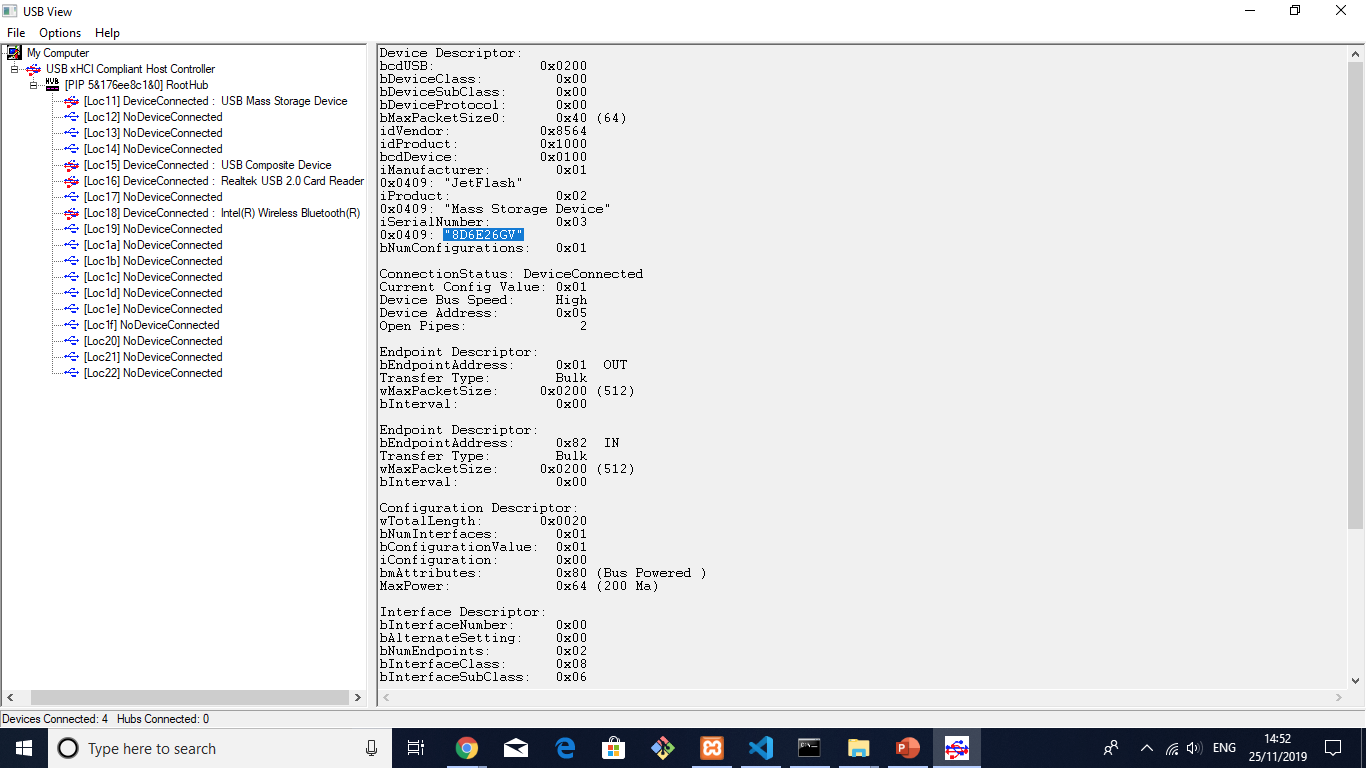
****

Figure . Matching USB serial number

Attempts to link the user to the USB after exploring the NTUSER.DAT file have failed, a list of most recently connected devices to the users account on the laptop should be visible but findings have come up short, the Volume information is blank.

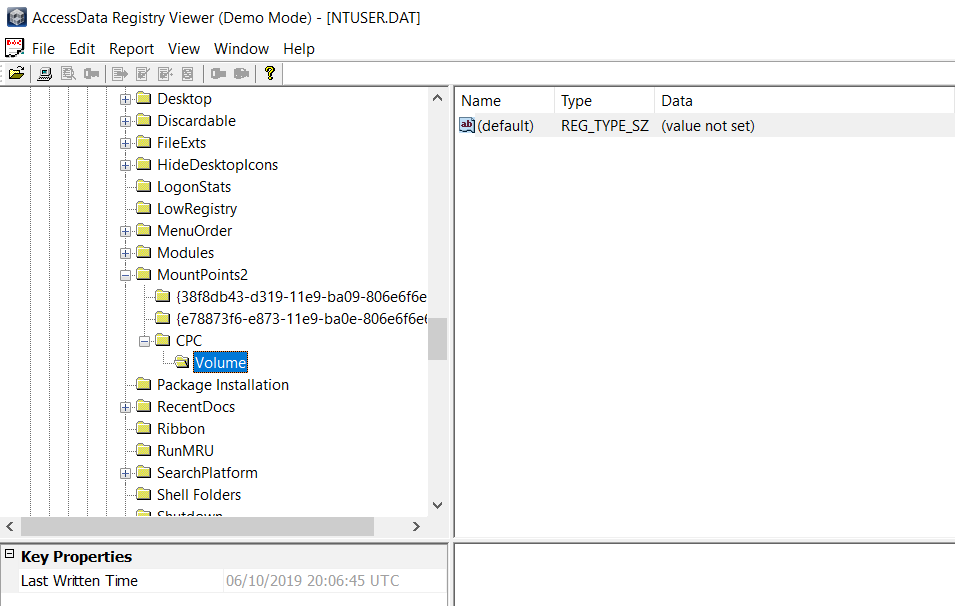


Figure . NTUSER.DAT inconclusive results

The following Event Log shows Logon and Logoff records and a Service shutdown record, additionally referring back to figure 4.8 shows a shutdown record on the laptop.

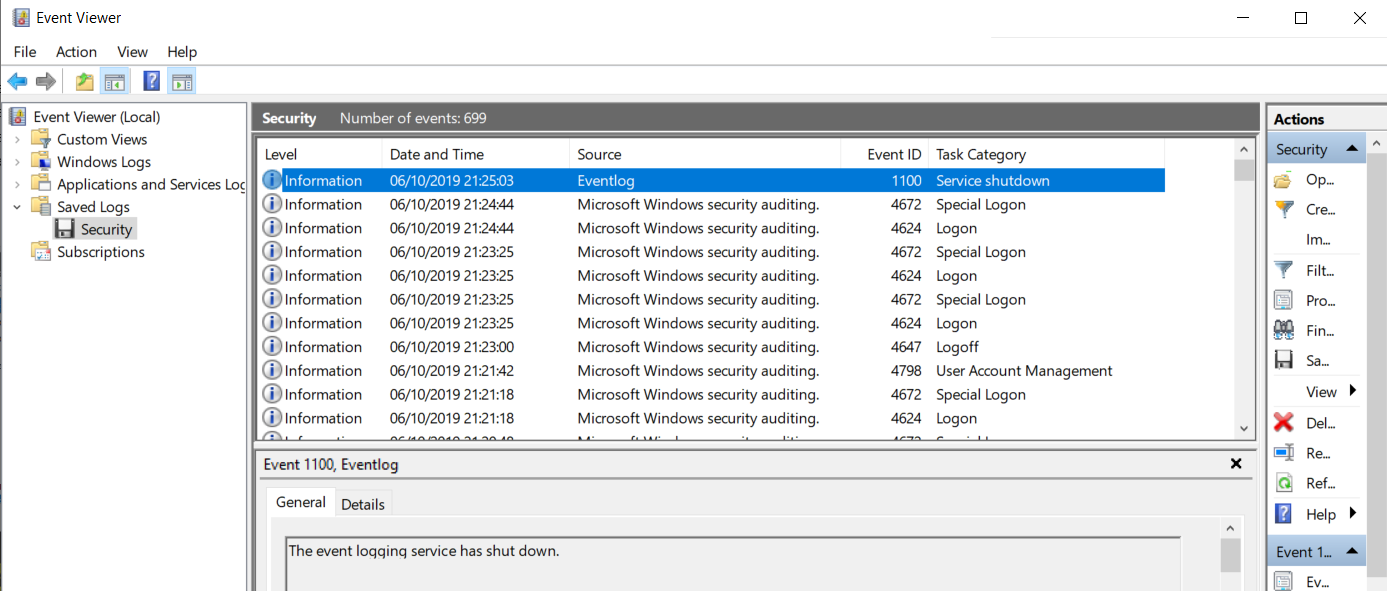


Figure . Logon, Logoff and shutdown records

Using WinPrefetchView it can be seen that the timeline matches up to MSAccess being opened during the time the laptop being investigated was being used by this potential malicious user.

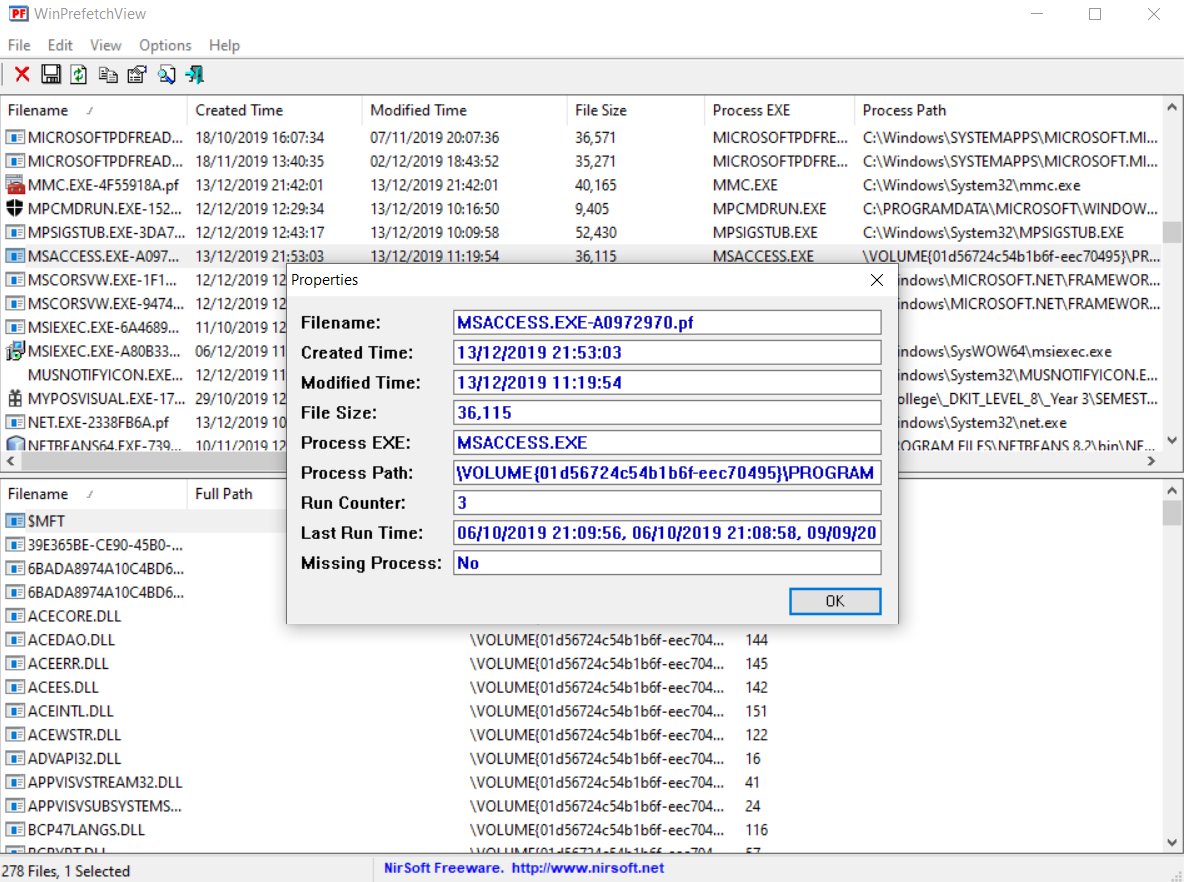


Figure . PrefetchView of the MSAccess.exe

The Following image shows the internet browsing history of the user FrancesWorkPC, stored in the web cache using the Microsoft Edge browser it is clear that the user has malicious intent for the data they stole from Mondial ltd, “selling customer data”, “how to sell data” and “sell data online” are three alarming results that have turned up.

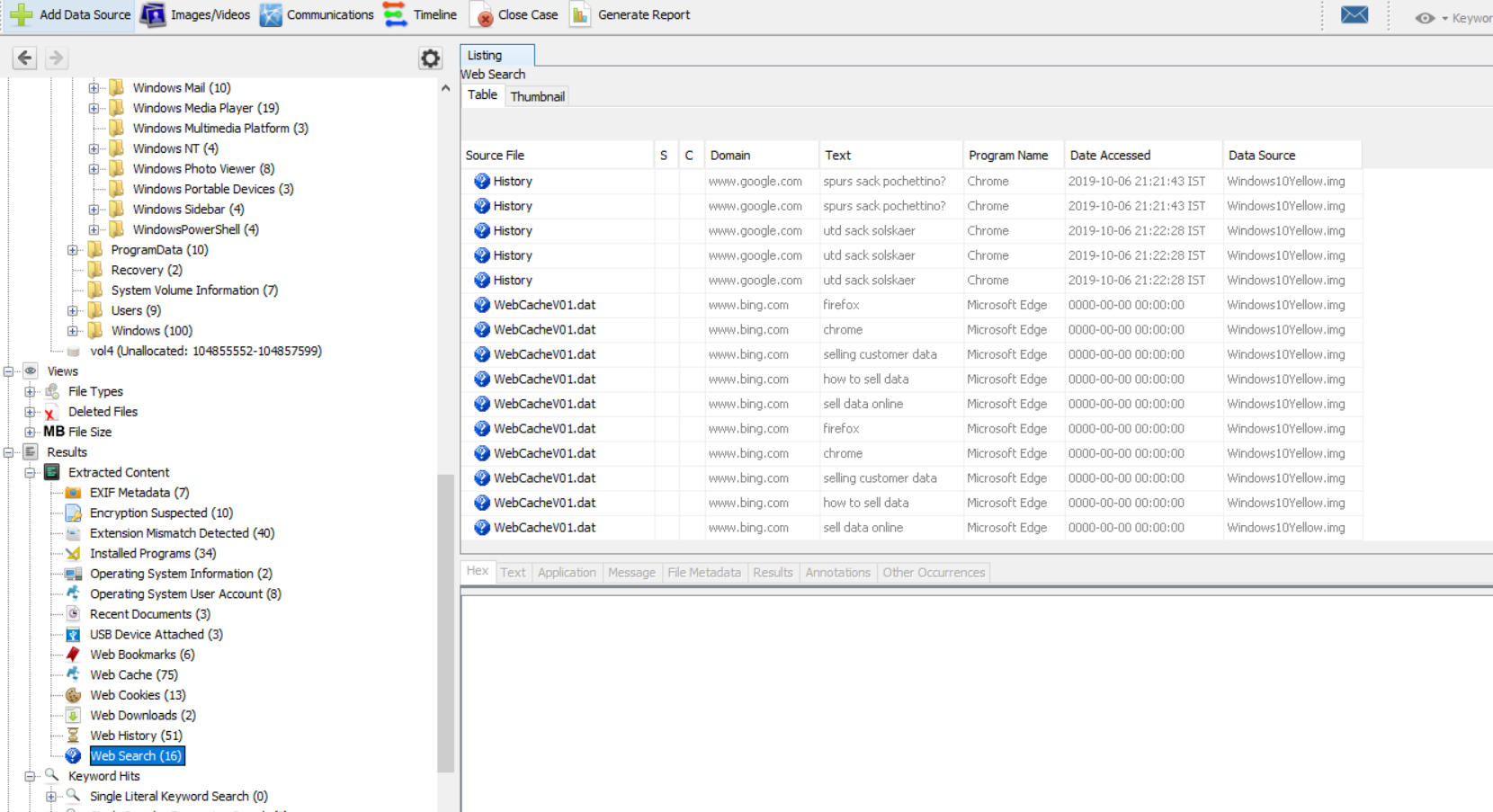


Figure . Evidence of malicious intent

# Conclusion

With all the evidence gathered in this report and in previous investigations, it is clear that the user behind the keyboard regarding this activity has malicious intent for the sensitive information stored in the database in Mondial ltd. The activities legality was already on the wrong side of the law, but now that the intent is clear, which is to sell this sensitive user data, the proper authorities must be contacted, if Mondial ltd are unwilling to follow through with this a representative of DigFor Inc will have to make this a police matter as failure to disclose this illegal activity to the police could reflect poorly on DigFor Inc and cause the company to become an accessory through the obstruction of justice.

The first person of contact should be Ms Frances Byrne as she is the owner of this account and as of this moment is the only known person to have access to this account, that is to say she is not by any means accused but is a prime suspect. Last time this employee was in discussion their whereabouts was unknown, if this is still the case the police must be contacted immediately as this individual could potentially be in serious danger.